UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,612	09/19/2003	Michael J. LaGasse	041-03us1	6407

36522 7590 06/12/2008

MAGIQ TECHNOLOGIES, INC
171 MADISON AVENUE, SUITE 1300
NEW YORK, NY 10016-5110

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
06/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/665,612	LAGASSE ET AL.	
	Examiner	Art Unit	
	JENISE E. JACKSON	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-8, 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoke et al(6,701,437) in view of Elliot(7,068,790), and further in view of Federal Information Processing Standards Publication 140-2.

3. As per claim 1, Hoke et al. discloses VPN(see col. 3, lines 27-28) having first(fig. 1 sheet 1, #140) and second VPN stations(see col. 3, lines 33-35, fig. 1 sheet 1 #150), a classical encryption system having first and second operatively connected encryption/decryption processors(see fig. 1 sheet 1, #115, #145, #155, col. 6, lines 27-40, 48-58, col. 7, lines 27-57) operatively connected to the first and second VPN stations(see col. 6, lines 48-57). Hoke does not disclose a quantum key distribution(QKD) system having first and second operatively connected QKD stations, the QKD system being adapted to exchange a quantum key between the first and second QKD stations and provide the quantum key, encrypt signal using the quantum key. Elliot discloses disclose a quantum key distribution(QKD) system(see col. 2, lines 7-12) having first and second operatively connected QKD stations(#105a, #105b see fig. 1 sheet 1), the QKD system being adapted to exchange a quantum key between the first and second QKD stations and provide the quantum key, encrypt signal using the quantum key(see col. 4, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the

invention to include Quantum Key Distribution(QKD) of Elliot with Hoke, the motivation is that by using QKD it assures the confidentiality of encryption keys distributed across a QKD path that may include multiple switches and links in a multi-mode QKD network(see col. 2, lines 14-20 of Elliot). Thus, the confidentiality of the distributed encryption key(s) assured, the privacy of any data encrypted using the distributed encryption key(s) is further assured(see col. 2, lines 14-23 of Elliot). Hoke nor Elliot disclose a Federal Information Processing Standards(FIPS). Federal Information Processing Standards(FIPS) teaches classical encryption is FIPS compliant, and teaches that level 1 includes encryption(see pg. 1). It would have been obvious to include the classical encryption is FIPS compliant, with Hoke-Elliot combination, the motivation is that by having a FIPS standard, it satisfies the cryptographic module utilized within a security system protecting sensitive information(see iii of FIPS 140-2).

4. As per claim 2, Hoke discloses first and second transmitting/receiving stations(see fig. 1 sheet 1, #140, #150) operatively connected to the first and second VPN stations(see col. 6, lines 48-57), respectively, wherein the first and second transmitting/receiving stations are adapted to transmit and/or receive plaintext(i.e. decrypt) signals to and from the respective first and second VPN stations(see col. 6, lines 27-40, 48-58, col. 7, lines 27-57).

5. As per claim 3, Hoke discloses the first and second e/d processors are connected by and Ethernet section(see col. 6, lines 20-26).

6. As per claim 4, Hoke discloses the first and second VPN stations are computers(see col. 6, lines 41-45).

7 As per claim 5, Hoke does not disclose a quantum key storage device for storing the quantum key provided by the QKD system. Elliot discloses a quantum key storage device for

storing the quantum key provided by the QKD system(see col. 4, lines 61-64).). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Quantum Key Distribution(QKD) of Elliot with Hoke, the motivation is that by using QKD it assures the confidentiality of encryption keys distributed across a QKD path that may include multiple switches and links in a multi-mode QKD network(see col. 2, lines 14-20 of Elliot). Thus, the confidentiality of the distributed encryption key(s) assured, the privacy of any data encrypted using the distributed encryption key(s) is further assured(see col. 2, lines 14-23 of Elliot).

8. As per claim 6, Hoke discloses a VPN layer(see fig. 1 sheet 1), a classical encryption layer connected to the VPN layer(see col. 6, lines 27-40, 48-58). Elliot discloses a QKD layer, wherein the QKD layer provides a quantum key to the classical encryption layer so that the classical encryption layer is capable of encryption information using the quantum key(see col. 4, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to include encryption using a quantum key of Elliot with Hoke, the motivation is that using a quantum key for encryption can detect eavesdropping on the QKD path/layer and my route the distribution of encryption keys around the eavesdropping in the network, and encryption by using a quantum key can also be used to locate if there is a eavesdropper(see col. 2, lines 25-31 of Elliot).

9. As per claim 7, Elliot discloses the QKD layer includes first and second QKD stations respectively operatively coupled to the first and second e/d processors and adapted to symmetrically distribution the quantum key to the first and second e/d processors(see col. 2, lines 7-12, fig. 1 sheet 1). It would have been obvious to one of ordinary skill in the art at the time of the invention to include encryption using a quantum key of Elliot with Hoke, the motivation is

that using a quantum key for encryption can detect eavesdropping on the QKD path/layer and my route the distribution of encryption keys around the eavesdropping in the network, and encryption by using a quantum key can also be used to locate if there is a eavesdropper(see col. 2, lines 25-31 of Elliot).

10. As per claim 8, Hoke discloses first and second transmitters/receivers operatively connected through a VPN(see fig. 1 sheet 1); encryption system col. 6, lines 27-40, 48-58, col. 7, lines 27-57). Elliot discloses a QKD system provides a quantum key to the encryption system to encrypt and decrypt a plaintext signal input from one of the first and second transmitters/receivers(see col. 2, lines 14-20, col. 4, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to include encryption using a quantum key of Elliot with Hoke, the motivation is that using a quantum key for encryption can detect eavesdropping on the QKD path/layer and my route the distribution of encryption keys around the eavesdropping in the network, and encryption by using a quantum key can also be used to locate if there is a eavesdropper(see col. 2, lines 25-31 of Elliot).

11. As per claim 9, Hoke nor Elliot disclose the classical encryption system is FIPS-compliant. Federal Information Processing Standards(FIPS) teaches classical encryption is FIPS compliant, and teaches that level 1 includes encryption(see pg. 1). It would have been obvious to include the classical encryption is FIPS compliant, with Hoke-Elliot combination, the motivation is that by having a FIPS standard, it satisfies the cryptographic module utilized within a security system protecting sensitive information(see iii of FIPS 140-2).

12. As per claim 10, limitations have already been addressed(see claims 1 and 7).

13. As per claim 11, limitations have already been addressed(see claim 2).

14. As per claim 12, limitations have already been addressed(see claim 3).

15. As per claim 13, Hoke discloses transmitting an encrypted signal between first and second transmitting/receiving stations(see col. 7, lines 27-46), sending a first plaintext signal from the first transmitting/receiving station to a first VPN station of a VPN; converting the first plaintext signal to a first VPN signal at the first VPN station; providing the first VPN signal to a first encryption/decryption processor of a classical encryption system also having a second processor(see col. 7, lines 27-58), forming an encrypted VPN signal from the first VPN signal at the first processor(see col. 7, lines 27-46), for a decrypted VPN signal from the encrypted VPN signal at the second processor(see col. 7, lines 27-58), forming second plaintext signal from the decrypted VPN signal at a second VPN station in the VPN; and receiving the second plaintext signal at the second transmitting/receiving station(see col. 8, lines 38-51, col. 9, lines 6-17).

16. Hoke does not disclose a quantum key. Elliot discloses exchanging a quantum key between first and second QKD stations in a QKD system and providing the quantum key to the first and second processors(see col. 4, lines 7-20); using the quantum key provided to the first processor; using the quantum key provided to the second processor(see col. 4, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to include encryption using a quantum key of Elliot with Hoke, the motivation is that using a quantum key for encryption can detect eavesdropping on the QKD path/layer and my route the distribution of encryption keys around the eavesdropping in the network, and encryption by using a quantum key can also be used to locate if there is a eavesdropper(see col. 2, lines 25-31 of Elliot).

17. As per claim 14, limitations have already been addressed(see claim 6).

18. As per claim 15, limitations have already been addressed(see claim 7).

19. As per claim 16, FIPS standard teaches forming the classical encryption link with a FIPS compliant encryption link(see pg. 1-2). It would have been obvious to include the encryption link is FIPS compliant, with Hoke-Elliot combination, the motivation is that by having a FIPS standard, it satisfies the cryptographic module utilized within a security system protecting sensitive information(see iii of FIPS 140-2).

.

Response to Applicant

20. The Applicant's response to Examiner's previous rejection on 101 is persuasive. Therefore, the 101 rejection has been withdrawn.

21. The Applicant states that Hoke nor Elliot disclose a VPN type communication system that uses FIPS and classical encryption. The Examiner disagrees with the Applicant. Hoke discloses the VPN traffic sent or received by endstations within headquarters LAN conform to a tunnel format. Data packets generated by an endstation in LAN are received by a VPN unit where they are encrypted and encapsulated within VPN packets addressed to the VPN unit serving the destination endstation(see col. 7, lines 47-57). Thus, Hoke discloses a VPN communication system that uses classical encryption. Hoke nor Elliot disclose the classical encryption system is FIPS-compliant. Federal Information Processing Standards(FIPS) teaches classical encryption is FIPS compliant, and teaches that level 1 includes encryption(see pg. 1). It would have been obvious to include the classical encryption is FIPS compliant, with Hoke-Elliot combination, the motivation is that by having a FIPS standard, it satisfies the cryptographic module utilized within a security system protecting sensitive information(see iii of FIPS 140-2).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 6, 2008

/J. E. J./

Examiner, Art Unit 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139